REMARKS

In this amendment, claims 7 to 10 and 16 have been cancelled without prejudice. Accordingly, the number of claims presented for examination have been reduced.

Claims 1 and 15 have been amended to make more clear that the public data is "received" and thereby clarify the differences between the prior art cited by the Examiner and the subject-matter of the present application. Because these claim amendments place this application in better form for appeal, this amendment should be entered after the final rejection.

The rejection of independent claim 7 (and claims 8 and 10 that depend on claim 7) as being anticipated by Doljack (US Patent 6,442,276) (and, with respect to claim 9 as being obvious) is moot in view of the cancellation of these claims.

The rejection of claims 1, 3 to 6 and 15 to 17 for obviousness of Doljack in view of Moore (US Patent 5,895,073) is traversed. [1]

Applicants submit that the combination of Doljack and Moore does not disclose at least the following the limitations of amended claim 1 the (most recent amendments are indicated by underlining):

> "receiving a request for verification,
> receiving the public data,
> generating a list of verification codes, each of said verification codes being generated by said predetermined

[1] The rejection of cancelled claim 16 is moot.

encryption algorithm by encrypting said received public data and one of said plurality of private data sets associated with the received public data, and

comparing said security code applied to the goods with said list of verification codes to assess the authenticity of goods"

Similar amendments have been made to independent 15. Claim 17 already stated that the public data was "obtained" which is similar to stating that the public data was received.

Doljack describes a method of verifying the authenticity of goods. In Doljack a random code is generated and then stored within a database (see Fig 2 and column 5 lines 55 to 57). When a good's authenticity needs to be verified, the code on the product is compared to the codes stored in the database (Step 70 Figure 2 Column 6 lines 33 to 37). This comparison determines whether the code is valid or not. Doljack further describes that the codes may be encrypted (See Figure 3 and associated description). To verify a code, the encrypted codes are decrypted and then compared to the codes stored in the database.

In contrast the invention as presently claimed, receives the public data that is to be verified, encrypts the public data and one of a plurality of private data sets to produce a verification code, and then compares the verification code to a security code to assess authenticity of the good.

Doljack does not disclose or suggest using the public data present on a good to produce a verification code that can be compared to a security code. Rather, the skilled person on reading Doljack would learn to transmit the security code to a verifier and decode it.

Moore discloses that marks or patterns on a good can be “compared directly to a set of authentic entries on a database or decoded and the decoded data compared to a set of data ” (Moore, Column 4). Nowhere does Moore disclose or suggest encrypting public data present on the goods to generate a code that should match a security code present on the goods if the goods are authentic.

In particular, Doljack (column 8, lines 15 to 16) describes "a method of verifying the authenticity of products without accessing an offsite master . . . .” In contrast, the present invention as presently claimed uses an offsite decryption algorithm to compare information derived from product packaging with other data to determine authenticity of the product. Doljack puts a single piece of information - a combination code - on the packaging. The "combination code" includes random and non-random data and is encrypted before being marked on the packaging. This is in direct contrast to the marking method recited in claim 7 which recites that “public data” be applied to the goods and a “security code” be applied to the goods. The security code of the present invention is derived from the public data "by means of a predetermined encryption algorithm".

With the methods and apparatus recited in independent claims 1, 15 and 17, the verification method and apparatus rely on encryption of the public data already on the goods which is passed back to a verification center having a verification database. This public data is received in the sense that it is read from the goods. Claim 1 further requires generating "a list of verification codes" using the public data on the goods, where "each of said verification codes being generated by said predetermined encryption algorithm by encrypting received said public data and one of said plurality of private data sets . . .". See also claims 15 and 17. The security code applied to the goods is then compared "with said list of verification codes to assess the authenticity of goods". In the present invention (as evident from claims 1, 15 and 17), it is only necessary to store the private data set which is relatively small. This private data set is able to generate a list of verification codes at will and as verification is required.

The step of generating a list of verification codes by encrypting received public data provided by the person wishing to verify the goods is not disclosed in Doljack. Furthermore, there is no storage of private data to operate with the encryption algorithm and no comparison with a list of verification codes.

Doljack fails to disclose goods having public data and a security code applied thereto. It fails to disclose the security code having been derived by means of a predetermined encryption algorithm by encrypting said public data, it fails to disclose generating a list of verification codes by re-encrypting said public data and one of said

plurality of private data sets and it fails to disclose comparing said security code with said list of verification codes.

In the system disclosed in Doljack, "public data on packaging", is not used to form the encrypted combination code. Doljack fails to disclose applying public data to the goods and applying a security code to the goods which is "derived by means of a predetermined encryption algorithm by encrypting said received public data . . .". Doljack does not disclose encrypting public data read from packaging. Doljack (column 8, lines 56 to 58) states that "the code on each tag will consist of only an encrypted counterpart . . ." and states at (column 8, line 62) that "the tags containing the encrypted combination codes are placed on products such that each product contains its own unique encrypted combination code . . .".

1. *Doljack Does Not Teach Marking Goods With A Security Code Derived From Received Public Data On The Goods.*

Doljack discloses the application of a single encrypted combination code which is not derived from public data applied to the goods. The obviousness rejection should be withdrawn for at least the reason that Doljack does not teach goods marked with a security code derived from public data marked on the goods and received via the goods.

Doljack (see column 9 at lines 9 to 16) relies primarily on decryption of a non-random code portion. This non-random code portion is the same for all products of the same type and because there is no encryption verification step as recited in claim 1 and because the nature of Doljack is that verification is carried out locally. Doljack matches

on a single non-random code. To do otherwise, would make the database requirements of Doljack unmanageable since a copy of every code would need to be stored on every local verification computer.

In connection with independent apparatus claim 15 and independent method claims 1 and 17, Doljack fails to disclose an apparatus or method for verifying the authenticity of goods having public data and a security code applied thereto, in which the security code has been derived by means of a predetermined encryption algorithm by encrypting said public data.

Furthermore, Doljack fails to disclose a processor as recited in claim 15 configured to generate a list of verification codes which are generated by said predetermined encryption algorithm by encrypting said public data and one of said plurality of private data sets. In addition, independent claims 1, 15 and 17 require the generation of lists of verification codes. Additionally, Doljack fails to disclose the process of comparing the security code applied to the goods with the list of verification codes to assess the authenticity of the goods. Independent claims 1, 15 and 17 require comparing the security code on the goods to the list of verification codes generated from the public data on the goods.

2. *Moore's Request For Verification Does Not Suggest Modifying Doljack To Form The Claimed Invention.*

Moore was applied as teaching a request for verification. Moore does not suggest the steps of claims 1, 15 and 17 regarding goods with both received public data and a

security code, where the security code is derived by encrypting the "received public data applied to the goods." It would not have been obvious to a person of ordinary skill in the art to combine Doljack and Moore to apply to goods the claimed public data and security code.

Moore does not suggest a security code derived from public data also printed on goods or a processor to generate verification codes from the printed public data. The combination of Doljack and Moore would not have rendered obvious the apparatus defined by claim 15.

The rejection of dependent claims 3 to 6 is also traversed for the same reason a stated above for independent claim 1.

The rejection of dependent claim 2 for obviousness is traversed for the same reasons that independent claim 1 is shown above to be patentable over Doljack and Moore.

All claims are in good condition for allowance. If any small matter remains outstanding, the Examiner is requested to telephone applicants' attorney. Prompt reconsideration and allowance of this application is requested.

The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Account No. 14-1140.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: /Jeffry H. Nelson/
Jeffry H. Nelson
Reg. No. 30,481

JHN:glf
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100